A FEDERAL CYBER CENTER

DC3 Department of Defense Cyber Crime Center

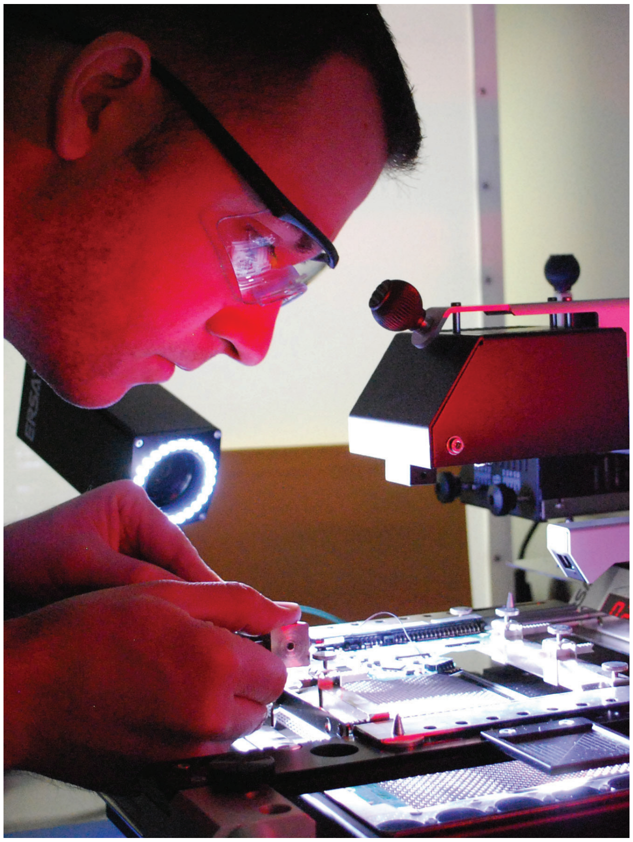
06/02/17

FACT SHEET

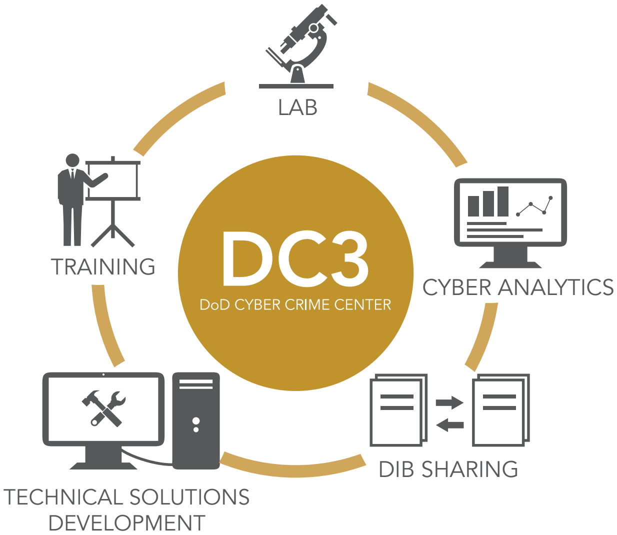
DoD CYBER CRIME CENTER (DC3)

Established as an entity within the Department of the Air Force in 1998, DC3 provides digital and multimedia (D/MM) forensics, specialized cyber training, technical solutions development, and cyber analytics for the following DoD mission areas: cybersecurity (CS) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT). DC3 delivers capability via six functional organizations which create synergies and enable considerable capability for its size.

DC3 is designated as a federal cyber center by National Security Presidential Directive 54 / Homeland Security Presidential Directive 23, as a DoD center of excellence for D/MM forensics by DoD Directive 5505.13E, and serves as the operational focal point for the Defense Industrial Base Cybersecurity Program (DIB CS Program; 32 CFR Part 236). DC3 delivers capability with a team of approximately 430 people, comprised of Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized staff support.



A DC3 lab specialist extracts data from damaged media: one of the most challenging but important services the lab provides. Photo by Al Fiterman



DC3 hosts liaisons from numerous mission partners, to include the Department of Homeland Security, the Office of the Under Secretary of Defense for Acquisitions, Technology, and Logistics (OUSD-AT&L) Damage Assessment Management Office (DAMO), National Security Agency, Federal Bureau of Investigation, DoD LE/CI organizations, U.S. Army Military Intelligence, and U.S. Cyber Command.

OPERATIONS

Defense Computer Forensics Laboratory (DCFL) -- DCFL performs D/MM forensic examinations, device repair, data extraction, and expert testimony for DoD. The lab's robust intrusion and malware analysis capability also supports other DC3 lines of business, and activities such as the OUSD (AT&L) DAMO. DCFL operations are accredited under ISO 17025 by the American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB) which guides reliable, repeatable and valid exam results, subjected to quality control and peer review.

Defense Cyber Investigations Training Academy (DCITA) -- DCITA provides classroom and web-based cyber training via more than 30 courses to DoD elements that protect DoD information systems from unauthorized, criminal, fraudulent, and foreign intelligence activities. DCITA confers DoD certifications in digital forensics and cyber investigations. To complement its in-residence training, DCITA has an extensive distance learning program (DCITA.edu). During FY17, DCITA delivered a combined total of 126,000 hours of training via classroom and online learning to students with duties in DoD LE/CI, cybersecurity analysis, and Cyber Mission Forces Cyber Protection Teams.

Analytical Group (AG) -- DC3's AG performs sharply focused technical analyses to support the cyber investigations and operations of LE/CI agencies, principal among them AFOSI, NCIS, and FBI. As a member of the National Cyber Investigative Joint Task Force (NCIJTF), the AG also leads collaborative analytical and technical exchanges with subject matter experts from LE/CI, cybersecurity, and the intelligence community (IC), to enable proactive LE/CI cyber operations focused on nation-state threat actors.

Department of Defense-Defense Industrial Base (DoD-DIB) Collaborative Information Sharing Environment (DCISE) -- As the operational hub for the DoD-DIB Cybersecurity Information Sharing Program, DCISE assists DIB companies to safeguard unclassified DoD information residing on or transiting their unclassified networks from nation-state threats. In this voluntary partnership, DCISE develops and shares actionable threat products, and performs cyber analysis and remediation consults for DIB Partners with DC3 lab support for malware analysis and intrusion forensics. Since FY08, DC3 has shared more than 160,000 intrusion indicators, performed 37,000 hours of malware analysis, and published more than 6,900 reports on significant cyber events of concern to the partnership. DC3 also serves as the single focal point for receiving all mandatory cyber incident reporting affecting the unclassified networks of DoD Contractors.

Defense Cyber Crime Institute (DCCI) -- As DC3's technical solutions development capability, DCCI tailors software and system solutions to support the AG, DCISE, and DCFL with tools and techniques engineered to the specific requirements of digital forensic examiners and cyber intrusion analysts. DCCI also develops tools such as DC3 "Advanced Carver" to aid data extraction for various DoD requirements such as DOMEX. On the test and evaluation side, DCCI validates COTS, GOTS, hardware and in-house developed software before use in a forensic process (a prerequisite for lab accreditation).

DoD Vulnerability Disclosure Program (DVDP) -- In late 2016, DoD established the DVDP as a broad and enduring capability to augment targeted and periodic "Bug Bounty" initiatives. The DVDP policy authorizes private-sector cybersecurity researchers to scan any and all public-facing DoD web sites at any time and provides a capability for reporting identified vulnerabilities to DC3. DC3 evaluates reported vulnerabilities and coordinates with Joint Forces HQ DoDIN for remediation by the website owner. DC3 validates the effectiveness of remediation actions and provides feedback to the researcher and trend analytics to DoD CIO.